

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE  
DIRECTORS OF THE DOD FIELD ACTIVITIES  
CHIEF INFORMATION OFFICERS OF THE MILITARY  
DEPARTMENTS  
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND  
COMPUTER SYSTEMS, JOINT STAFF  
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES  
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF  
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER  
COMMANDERS OF THE UNIFIED COMBATANT COMMANDS

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 10-8460 -  
Network Operations -

The attached Department of Defense and Intelligence Community Network Operations guidance and policy will become effective after an initial concept demonstration within USPACOM. The implementation is also contingent upon the development and approval of the DoD network management component of the Enterprise Wide Network Architecture (EWNA).

The policy that follows is intended to place an operational focus on the management of the Global Information Grid. It establishes C4I network management and network defense activities as ongoing military operations under the Combatant Command authority of the CINC. This operational hierarchy will oversee control and management capabilities that will achieve end-to-end distributed control while providing a common view and joint use of management information.

This policy guidance will apply initially to USPACOM, its Components, and other DoD organizations operating in its AOR. This is intended to demonstrate the feasibility and utility of proposed organizational and procedural constructs within the USPACOM theater. Upon conclusion and subsequent after action reviews, I will direct the Senior Civilian Official for C3I to incorporate the attached policy guidance into the DoD Directive System.

My point of contact for this effort is Mr. Gary Demas who can be reached at (703) 607-0664, or by e-mail: gary.demas@osd.pentagon.mil. The Joint Staff POC is COL Gary Kollmann at DSN 224-4072, or gary.kollmann@js.pentagon.mil.

<signature block for John Hamre>

# **Guidance and Policy for the Department of Defense and Intelligence Community Network Operations**

## **1. PURPOSE**

This Guidance and Policy Memorandum (G&PM) establishes Department of Defense (DoD) policy to enable the secure exchange and use of information necessary to the execution of the DoD mission. This issuance establishes policies, guidance and assigns responsibilities to:

- 1.1. Establish C4I network management and network defense as ongoing military operations.
- 1.2. Institutionalize C4I networks as warfighting resources under CINC Combatant Command authority.
- 1.3. Implement positive control and security of networks through a network operational hierarchy.
- 1.4. Implement control and management capabilities that achieves end-to-end distributed control while providing a common view and joint use of management information.
- 1.5. Provide the Unified CINCs network situational awareness.
- 1.6. Provide the Unified CINCs authoritative direction over network resources, in coordination with DISA, as a function of the Global Information Grid.

## **2. APPLICABILITY**

2.1. This guidance and policy applies to the Office of the Secretary of Defense, the Military Departments, and their respective Services, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as “the DoD Components”).

2.2. This policy must comply with public law and established DoD and Director Central Intelligence (DCI) Directives relative to architecture, acquisition and security policies and practices.

2.3. Intelligence Community (IC) SCI networks and the organizations required to manage them will be considered resources supporting both warfighting and other national interests. As such, they will remain under the control of their respective transport and service network manager, to the extent necessary to provide protection unique to intelligence information that exceeds that provided by DoD designated

operations centers. These resources will also remain under IC control to ensure that there is no conflict with other National mission requirements. As such, the IC will ensure that CINC requirements for IC network situational awareness are met.

### **3. SCOPE**

Policy that follows is intended to place an operational perspective on the management of networks. Detailed network, systems and applications management will be addressed in follow-on instructions or doctrinal publications, or in revisions to existing publications. In addition, Information Assurance and Information Dissemination Management are presently addressed in separate guidance and policy memorandums.

### **4. DEFINITIONS** See Enclosure

### **5. POLICY**

5.1. DoD will execute Enterprise Operations through a hierarchy that distributes management and control functions, while integrating operational oversight. DoD components will exercise routine, day-to-day management and control of their designated Enterprise service and transport network elements. CINCs will oversee and coordinate management activities within their theaters. The CJCS, through the Joint Staff and appropriate authorities (e.g. CND JTF (USSPACECOM) for network security) will adjudicate issues involving the operational network environment.

5.2. DoD will develop a joint network management operational and systems architecture consistent with the C4ISR Architecture Framework, as a component to the Enterprise-Wide Network Architecture (EWNA). These architecture views will describe in detail how DoD components will visualize, monitor, control, and/or manage networks to sustain the Global Information Grid.

5.3. DoD Components will implement standardized, interoperable control and management capabilities for their networks, consistent with the EWNA.

5.4. DoD Components will exercise management and control of their designated Enterprise service and transport network elements within a tiered management hierarchy consisting of global, regional, and local Network Operations and Security Centers (NOSCs).

5.5. DoD Components will integrate their network management, information assurance, and information dissemination management activities.

5.6. DoD Components designated as Enterprise service network managers by the DoD CIO Executive Board will be given end-to-end visibility for their service across all other DoD component transport networks as described in the EWNA.

5.7. Enterprise service network managers will provide the required visibility detailed in the EWNA to facilitate global, as well as regional network situational

awareness. (This provides DISA, the Joint Staff, and the CINCs the requisite network situational awareness to perform their joint oversight role. In cases where Unified CINCs are not supported by a DISA regional NOSC, the CINC may designate a particular component NOSC to receive this information.)

5.8. CINCs will have a network Common Operational Picture (COP) for their AOR provided by a supporting DoD component NOSC consistent with the EWNA. All DoD components will provide the designated NOSC with information concerning the status and condition of their networks, necessary to create and maintain the network common operational picture (COP).

5.9. Service and transport networks designated as part of the DoD/IC Enterprise Network, along with the organizations required to manage them, will also be designated “forces” necessary for the performance of military missions.

5.10. The Combatant CINC will have Combatant Command (COCOM) authority over those transport network resources, to include regional operations centers, within his AOR, consistent with Title X. In exercising this authority, CINCs will be cognizant of Service and Agency support to the NCA, their respective organizations, and other CINCs, and will preserve GIG integrity and standards.

5.11. CINCs can delegate Operational Control (OPCON) and/or Tactical Control (TACON) authority over regional operations or local control centers, to subordinate commands or other DoD Components operating in their AOR, consistent with their Title X authority. This provides CINCs the authority to determine how network situational awareness data within their theaters will be aggregated, as well as the authority to resolve issues which cross component management boundaries. Operational area extensions to IC (SCI) networks will come under tactical control of the CINC through the CINC J2 and J6.

5.12. Governance will focus on functions associated with architecture and policy development and implementation; corresponding issue resolution; and acquisitions and funding. Governance will be distinct from operations management.

## **6. RESPONSIBILITY**

6.1. Assistant Secretary of Defense (C3I)/DoD CIO:

6.1.1. Promulgate and issue guidance and instructions to this policy.

6.1.2. Promulgate GNIE overarching policy

6.2. Chairman of the Joint Chiefs of Staff:

6.2.1. Provide management direction involving the allocation of network resources, including the arbitration of resources between CINCs.

6.2.2. Develop, in collaboration with CINCs, Services, and Agencies, common network operations tasks, to include but not limited to fault, configuration,

accounting, performance, and security management, for inclusion into the Universal Joint Task List (UJTL).

6.2.3. Develop and publish standardized DoD procedures for network operations tasks as established above.

6.3. Commander, Computer Network Defense Joint Task Force (CND JTF):

6.3.1. Will remain DoD's primary operations center, collocated with the DISA Global Network Operations and Security Center (GNOSC), to monitor and respond to attacks and intrusions against the Global Information Grid.

6.3.2. Will coordinate and direct computer network defense activities which cross CINC boundaries.

6.4. Commander in Chief (CINCs) Unified Commands:

6.4.1. Will determine, in collaboration with DISA and their respective Service Component Commands, the reporting requirements necessary to create and maintain a network Common Operational Picture (COP).

6.4.2. Will develop a Concept of Operation delineating their subordinate command relationships with regard to network operations, and supplemental guidance for the performance of associated tasks, consistent with established standardized DoD procedures.

6.4.3. When designated a supporting CINC, provide network visibility to the supported CINC, for those supporting CINC unique networks deemed critical by the supported CINC.

6.5. IC CIO:

6.5.1. Will collaborate in the development of the joint network management architecture.

6.5.2. Has programmatic responsibility for acquiring and maintaining standards-based network management systems IAW the EWNA.

6.5.3. Will provide network visibility directly to the CINC.

6.5.4. Will develop a roadmap to be executed within 5 years from the date of this policy to provide IC/SCI network status directly to the CINC's supporting NOSC.

6.5.5. Will coordinate network operations activities directly with the theater CINC J2 and J6.

6.6. Military Departments and Defense Agencies:

6.6.1. Have programmatic responsibility for acquiring and maintaining standards-based network management systems IAW the EWNA.

6.6.2. Will evaluate the requirement to status and control legacy network elements, and will ensure that all future components to the Global Information Grid are

fielded with an embedded capability to be monitored and controlled remotely, consistent with the developed architecture.

6.6.3. Will establish a global Network Operations and Security Center (NOSC), as appropriate, to serve as a central point of contact in operational matters concerning the DoD Component's portion of the GIG, and will share network situational awareness data with DISA's Global NOSC. The global NOSC will also serve as a central point of contact in operational and emergency provisioning aspects for the CINC, when the needs are beyond the capability of the regional NOSCs.

6.6.4. Will establish regional NOSCs, as appropriate, to provide a single point of contact for the theater DoD component for network services, operations status, and anomalies. They may also serve as a central point of contact for operational matters in support of a theater CINC.

6.6.5. Will establish Local Control Centers (LCC), as appropriate, to manage and control networks and services either deployed or fixed at the base, post, camp, or station. The LCCs provide the "first line" of problem resolution and are the primary points of contact concerning reliability and availability of managed C4I resources.

6.6.6. Will perform day-to-day management tasks associated with fault, configuration, accounting (including provisioning), performance, and security management on their designated service and transport networks, consistent with DoD and CINC guidance.

6.6.7. Will plan and program consolidation of network management, information assurance (to include Computer Emergency Response Team (CERT)), and Information Dissemination Management (IDM) capabilities into an organization consistent with the tiered hierarchy prescribed by this policy.

6.6.8. Will provide network visibility to DISA regional operations centers, or other DoD Component NOSCs, in accordance with CINC guidance, in order to create the CINC's theater-wide network picture.

6.6.9. Will provide service network visibility to the service network manager. (e.g. As DoD's SIPRNET manager, DISA will be provided visibility into Service (Army, AF, Navy etc.) network assets which extend SIPRNET service into the Military Departments.)

6.7. Defense Information Systems Agency (DISA). In addition to those responsibilities directly above, DISA will:

6.7.1. Advise the Joint Staff-J6 and CND JTF on matters regarding the allocation of network resources, outages, attacks and intrusions impacting the GIG. In support of this goal, DISA will maintain a global "roll-up" of the DoD network common operational picture.

6.7.2. Disseminate Joint Staff-J6 and CINC guidance and direction regarding management of the GIG to other DoD Components. This includes tasks which must be coordinated across service delivery points or demarcation lines associated with the control of network resources.

6.7.3. Coordinate the provisioning and maintenance of "transport" for service networks across multiple transport networks. As such, DISA will serve as the

single point of contact for service network managers when they need to provision and maintain service connectivity across multiple transport networks.

6.7.4. Lead the development of the joint network management architecture component of the EWNA, in collaboration with the CINCs, Services, and Agencies.

6.7.5. Lead all engineering efforts related to the integration and/or modernization of transport and service networks designated as a part of the DoD/IC Enterprise Network.

6.7.6. Revise reporting requirements and structures (i.e. Facility Control Offices) for the Global Information Grid in consonance with the developed architecture and CINC requirements.

6.7.7. Support the CINC in the creation of a network Common Operational Picture (COP) for his AOR. For those CINCs not directly supported by a DISA regional NOSC, coordinate with the CINC designated NOSC to provide the necessary information. (i.e. SOUTHCOM)

#### 6.8. Military Communications-Electronics Board (MCEB):

6.8.1. Will chair a Configuration Control Panel for deployed components to the DoD/IC Enterprise.

6.8.2. Oversee and coordinate the development of the deployed network management architecture in collaboration with CINCs, Services, and Agencies. Make recommendations to the DoD CIO Executive Board and the Architecture Coordinating Council.

6.8.3. Oversee tactical joint interoperability.

6.8.4. Coordinate the planning, design, resourcing, acquisition, and synchronization for systems in support of deployed networks through the DoD CIO Executive Board and the Architecture Coordinating Council.

### 7. EFFECTIVE DATE:

This policy is effective upon development and approval of the overall DoD network management architecture.

## **Appendix A: Definitions**

Enterprise Service Network: A DoD/IC-funded service network which has been designated by the governing structure as an “Enterprise Service Network” because it: 1) provides a unique, defined capability (e.g., functionality [packet data, switched voice, etc.], security, service assurance, interoperability, network operations, etc.), 2) is required by multiple DoD/IC components, 3) is consistent with an established DoD/IC architecture (the Enterprise-Wide Network Architecture, or EWNA), 4) is managed as a single entity, and 5) provides service to any user with a validated and funded requirement consistent with the defined capability of that service network.

Enterprise Service Network Manager: For a given Enterprise Service Network, a DoD/IC Component is tasked to manage service end-to-end. The service network manager must coordinate with those transport network providers whose resources are used to provide the end-to-end service.

Enterprise Transport Network: A DoD/IC-funded transport network, which has been designated by the governing structure as an “Enterprise Transport Network” because it provides the underlying capabilities for one or more Enterprise Service Networks.

Enterprise Transport Network Provider: For a given Enterprise Transport Network, a DoD/IC Component is tasked to provide connectivity for use by Enterprise Service Networks. The transport network provider must coordinate with those service network managers that use transport network resources.

Visibility is having the awareness of the status of a resource. It may or may not involve actually monitoring the resource.

Monitoring a resource requires the ability to communicate directly with the resource and receive “status” related information.

Control of the resource implies an ability to monitor the resource, but also includes the ability to manipulate the functioning of that resource, or allocate it to a specific use. The most common example of that capability is the term “configuration.” Both monitoring and control functions require the exchange of information or data between the resource and the organization with a particular interest in that resource. DISA’s Joint DII Control System (JDIICS) concept explains in greater detail this management information exchange.

Management of C4I resources is the ability to make decisions concerning the operation and/or maintenance of that resource. It does not necessarily imply the capability to see and control it.

Combatant Command (COCOM) authority is nontransferable command authority established by title 10 exercised only by commanders of unified or specified combatant

commands unless otherwise directed by the President or the SECDEF. COCOM cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. (Joint Pub 1-02)

Operational Control (OPCON) authority is transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational Control (OPCON) is inherent in COCOM. OPCON may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. (Joint Pub 1-02)

Tactical Control (TACON) authority is command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and usually local direction and control of movements or maneuvers necessary to accomplish missions or tasks. Tactical Control is inherent in operational control. Tactical Control may be delegated to, and exercised at, any level at or below the level of combatant command. (Joint Pub 1-02)

Coordinating Authority to require consultation between two or more Military Departments or two or more forces of the same Service by a commander or individual assigned responsibility for coordinating specific functions. It is not the authority to compel agreement. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. (Joint Pub 1-02)

Network Operations is an organizational and procedural framework which will provide the CINC J6 the means to effectively execute CINC priorities, while at the same time fulfilling management tasks identified to sustain the Global Information Grid. This framework will integrate the related functions of Network Management, Information Assurance, and Information Dissemination Management. In addition, the management tasks associated with the following areas are a part of Network Operations:

- |                                    |                                  |
|------------------------------------|----------------------------------|
| <del>✍</del> Bandwidth             | <del>✍</del> Global Applications |
| <del>✍</del> Spectrum              | <del>✍</del> Tactical Access     |
| <del>✍</del> Leased communications | <del>✍</del> Tactical Data Link  |
| <del>✍</del> Broadcast Networks    |                                  |

**GLOBAL NETWORKED INFORMATION ENTERPRISE (GNIE)**  
**Enterprise Operations Thrust Area**  
**Network Management/Organizations/C2 Panel Membership**

LAST	FIRST	RANK	ORGANIZATION	PHONE	E-MAIL
Bolling	Tom	GS-15	DISA DISN PM (D21)	703-681-0296	Bollingt@ncr.disa.mil
Coram	Jo	CIV	MITRE	703-883-7733	<a href="mailto:Jcoram@mitre.org">Jcoram@mitre.org</a>
Demas	Gary	GS-15	ASD (C3I)	703-607-0664	Gary.demas@osd.mil
Edelman	Sam	LTC	HQDA ODISC4	703-614-6166	Edelmsl@hqda.army.mil
Edwards	David	CIV	MITRE	703-883-7787	<a href="mailto:Edwards@mitre.org">Edwards@mitre.org</a>
Goldschmidt	Lee	CIV	MITRE/Navy SPAWAR	703-883-5213	<a href="mailto:lfgolds@mitre.org">lfgolds@mitre.org</a>
Kaylor	Henry	LTC	NGB AIS	703-607-7651	kaylohw@hqda.army.mil
Kollman	Gary	COL	JCS	703-614-4072	gary.kollman@js.pentagon.mil
Machabee	Larry	Col	CNO N61B	703-604-6880	larry.machabee@osd.mil
Morgan	Lou	GS-14	DISA/D3	703-607-6687	<a href="mailto:Morganl@ncr.disa.mil">Morganl@ncr.disa.mil</a>
Silberberg	David	GS-13	NSA	301-688-5931	<a href="mailto:Dsilber@romulus.ncsc.mil">Dsilber@romulus.ncsc.mil</a>
Tiddy	Mike	Capt	USMC	703-607-5699	<a href="mailto:Tiddyme@hqmc.usmc.mil">Tiddyme@hqmc.usmc.mil</a>
Wallace	Bill	CIV	DLA	703-767-3129	<a href="mailto:Bwallace@hq.dla.mil">Bwallace@hq.dla.mil</a>
Wech	Kim	CIV	DIA	202-231-5067	<a href="mailto:Afwelkr@dia.osis.gov">Afwelkr@dia.osis.gov</a>
Zdeb	Tanya	CIV	AFCIC SYNT	703-588-6147	tanya.zdeb@pentagon.af.mil
Totten	Eve	CIV	DFAS	703-607-3957	<a href="mailto:Ev.totten@dfas.mil">Ev.totten@dfas.mil</a>